

Cited Reference

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-134497

(43) 公開日 平成11年(1999) 5月21日

(51) Int.Cl.⁶

G 0 6 T 7/00

識別記号

F I

G 0 6 F 15/62

4 6 0

審査請求 未請求 請求項の数 7 O L (全 7 頁)

(21) 出願番号 特願平9-293820

(22) 出願日 平成9年(1997)10月27日

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 小野 剛

東京都千代田区東神田2丁目8番11号 ア

トミック株式会社内

(72) 発明者 塚村 善弘

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(72) 発明者 船橋 武

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

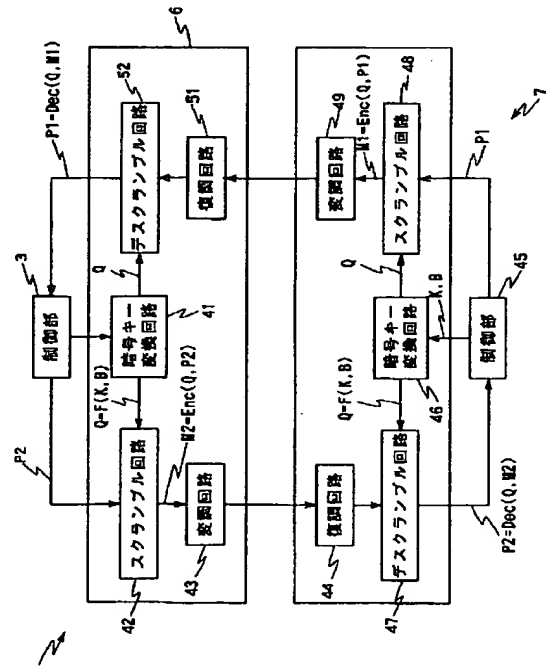
(74) 代理人 弁理士 多田 繁範

(54) 【発明の名称】 画像照合装置、画像照合システム、照合装置及び照合システム

(57) 【要約】

【課題】本発明は、画像照合装置、画像照合システム、照合装置及び照合システムに関し、例えば画像読み取り手段と照合手段とを一体化した構成においても、十分なセキュリティを確保できるようにする。

【解決手段】照合結果P2等を暗号化して出力するようにし、この暗号化に使用する暗号キーQをパラメータK、Bの伝送により更新する。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】照合対象の画像を入力する画像入力手段と、
前記照合対象の画像と所定の基準画像とを照合して照合結果を出力する画像照合手段と、
前記照合結果を外部機器に出力する通信手段とを備え、
前記通信手段は、
所定の暗号キーにより前記照合結果を暗号化して出力し、
前記外部機器より伝送されるパラメータより、前記暗号キーを更新することを特徴とする画像照合装置。

【請求項2】前記通信手段は、
従前の暗号キーにより前記外部機器より入力した入力データを処理して前記パラメータを取得することを特徴とする請求項1に記載の画像照合装置。

【請求項3】前記通信手段は、
従前の暗号キーにより前記外部機器より入力した入力データを処理してデータ列を得、前記データ列に付加された位置データに基づいて、前記データ列を選択的に取り込んで前記パラメータを取得することを特徴とする請求項1に記載の画像照合装置。

【請求項4】照合対象の画像を入力する画像入力手段と、前記照合対象の画像と所定の基準画像とを照合して照合結果を出力する画像照合手段と、所定の暗号キーにより暗号化して前記照合結果を外部機器に出力する通信手段とを有する端末機器と、
前記外部機器とを有する画像照合システムであって、
前記外部機器は、
前記暗号キーの生成に必要なパラメータを、従前の暗号キーにより暗号化して前記端末機器に送出し、
前記端末機器は、
前記パラメータを取得し、該取得したパラメータにより前記従前の暗号キーを更新することを特徴とする画像照合システム。

【請求項5】前記端末機器は、
前記パラメータに、冗長なデータ、前記パラメータの位置を示す位置データ、ランダムなデータを付加して伝送することを特徴とする請求項4に記載の画像照合システム。

【請求項6】照合対象のデータを入力する入力手段と、前記照合対象のデータと所定の基準データとを照合して照合結果を出力する照合手段と、
前記照合結果を外部機器に出力する通信手段とを備え、
前記通信手段は、
所定の暗号キーにより前記照合結果を暗号化して出力し、
前記外部機器より伝送されるパラメータより、前記暗号キーを更新することを特徴とする照合装置。

【請求項7】照合対象のデータを入力する入力手段と、前記照合対象のデータと所定の基準データとを照合して

照合結果を出力する照合手段と、所定の暗号キーにより暗号化して前記照合結果を外部機器に出力する通信手段とを有する端末機器と、

前記外部機器とを有する照合システムであって、
前記外部機器は、
前記暗号キーの生成に必要なパラメータを、従前の暗号キーにより暗号化して前記端末機器に送出し、
前記端末機器は、
前記パラメータを取得し、該取得したパラメータにより前記従前の暗号キーを更新することを特徴とする照合システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、画像照合装置、画像照合システム、照合装置及び照合システムに関し、例えばユニット化した端末機器により指紋照合する場合に適用することができる。本発明は、暗号キーにより暗号化して照合結果を伝送し、パラメータの伝送によりこの暗号キーを更新することにより、例えば画像読み取り手段と照合手段とを一体化して端末機器を構成した場合においても、十分なセキュリティを確保できるようにする。

【0002】

【従来の技術】従来、この種の画像照合装置でなる指紋照合装置においては、撮像手段を介して指紋の画像を読み取り、この指紋の画像より指紋の分岐、点、切れ等の特徴的な部分を抽出することにより、この特徴的な部分を基準にして指紋照合するようになされている。

【0003】

【発明が解決しようとする課題】ところでこの種の指紋照合装置において、画像読み取り手段でなる撮像手段、指紋照合処理を実行する演算処理手段等を一体化、小型化してユニット化すれば、例えば部屋の入退出管理等に適用できると考えられる。

【0004】ところがこのようにユニット化すると、このユニットと外部機器との間で照合結果を伝送することになり、この照合結果に対する不正な行為により、システムの安全性、信頼性が損なわれる問題がある。特に、このようなユニットと外部機器とを電話回線等の伝送路により接続する場合には、特にこの種の不正が問題となる。

【0005】本発明は以上の点を考慮してなされたもので、例えば画像読み取り手段と照合手段とを一体化した構成においても、十分なセキュリティを確保することができる画像照合装置、画像照合システム、照合装置及び照合システムを提案しようとするものである。

【0006】

【課題を解決するための手段】かかる課題を解決するため本発明においては、端末機器においては、所定の暗号キーにより照合結果を暗号化して出力し、外部機器より

伝送されるパラメータよりこの暗号キーを更新する。

【0007】また端末機器と外部機器とを有する画像照合システムにおいて、外部機器より、暗号キーの生成に必要なパラメータを、従前の暗号キーにより暗号化して端末機器に送出し、端末機器においては、このパラメータを取得し、該取得したパラメータにより従前の暗号キーを更新する。

【0008】また照合装置及び照合システムに適用して、外部機器より伝送されるパラメータより暗号キーを更新する。

【0009】照合結果を暗号化して伝送し、この暗号化の暗号キーを更新することにより、暗号キーの不正な取得に対応することができる。このとき外部機器より伝送されるパラメータよりこの暗号キーを更新すれば、暗号キー自体を伝送することを要しないことにより、暗号キーの不正取得を防止することができる。

【0010】

【発明の実施の形態】以下、適宜図面を参照しながら本発明の実施の形態を詳述する。

【0011】(1)全体構成

図2は、本発明の実施の形態に係る指紋照合装置を示すブロック図である。この指紋照合装置1は、生体検出部2、制御部3、指紋読み取り部4、画像照合部5、入出力部6が小型に一体化されたユニットにより構成される。指紋照合装置1は、このユニットが所定位置に配置されると共に、パーソナルコンピュータ等の外部機器7に接続され、例えば部屋の入退出管理等に適用される。

【0012】この指紋照合装置1において、生体検出部2は、所定の指載置位置に指が載置されると、制御部3に通知する。

【0013】指紋読み取り部4は、制御部3の制御によりこの指載置位置に載置された指の画像を撮像し、ビデオ信号SVを出力する。

【0014】画像照合部5は、制御部3の制御により動作モードを切り換え、このビデオ信号SVを2値化して画像データを生成する。また画像照合部5は、指紋登録モードにおいて、この指紋データD1、又は入出力部6を介して入力される指紋データを内蔵のデータベースに登録する。これにより画像照合部5は、この指紋登録モードにおいて、指紋照合の基準となる基準画像を登録する。

【0015】また指紋照合モードにおいて、このようにして内蔵のデータベースに登録した基準画像と、所定の指紋データによる指紋画像と照合し、照合結果を出力する。ここでこの指紋照合装置1において、指紋照合モードは、生体検出部2の検出結果をトリガにして、画像照合部5に保持した基準画像と指紋読み取り部4を介して得られる指紋画像とを照合する第1の自己照合モードと、外部機器7の指示をトリガにして画像照合部5に保持した基準画像と指紋読み取り部4より得られる指紋画

像とを照合する第2の自己照合モードと、外部機器7の指示により画像照合部5に保持した基準画像と外部機器7より入力される指紋画像とを照合する第2の外部照合モードとにより構成される。

【0016】画像照合部5は、これら3つの指紋照合モードに対応して、それぞれ指紋読み取り部4を介して得られる指紋画像、入出力部6を介して外部機器7より入力される指紋画像を照合対象に設定して、データベースに保持した基準画像との間で指紋照合の処理を実行する。

【0017】入出力部6は、制御部3の制御により、外部機器7より入力される制御コマンドを制御部3に通知し、また外部機器7より入力される画像データを画像照合部5に出力し、さらに画像照合部5による照合結果を外部機器7に出力する。

【0018】制御部3は、この指紋照合装置1全体の動作を制御するマイクロコンピュータにより構成され、外部機器7の制御により動作モードを設定する。

【0019】(1-1)入出力部の処理

図1は、指紋照合装置1の入出力部6と外部機器7との接続を示すブロック図である。この指紋照合装置1においては、外部機器7との間で入出力する各種データを図3に示すフォーマットによるメッセージP1及びP2に変換し、このメッセージP1及びP2を暗号化して伝送する。

【0020】すなわち制御部3は、外部機器7に対して、ステータス、照合結果等を送出する場合に、このステータス、照合結果をメッセージ部に割り当てて所定のパケットを形成する。このとき制御部3は、このパケットに冗長なデータを割り当てて一定のデータ量に設定した後、メッセージ部の位置を示す位置データ、ランダムなデータを割り当てる。これにより制御部3は、このパケットによるメッセージP1を所定の暗号キーによりスクランブル処理し、いわゆるSALTの手法により同一のメッセージ部を送出する場合でも、その都度異なるデータにより送出的ようになされている。

【0021】すなわち入出力部6において、暗号キー変換回路41は、制御部3より出力されるオリジナルパラメータK、変換パラメータBを受け、これらのパラメータB、Kより所定の演算処理を実行することにより暗号キーQ(=F(K, B))を生成する。なおここでF(K, B)は、パラメータB、Kより暗号キーQを作成する関数である。

【0022】スクランブル回路42は、制御部3より出力されるメッセージP2をこの暗号キーQ(=F(K, B))によりスクランブル処理し、これにより暗号化データM2(=Enc(Q, P2))を生成する。なおここでEnc(Q, P2)は、暗号キーQによりメッセージP2を暗号化する関数である。

【0023】変調回路43は、スクランブル回路42よ

り出力される暗号化データをシリアルデータ列に変換した後、この指紋照合装置1が外部機器と接続される伝送路に適した変調方式により、変調して出力する。

【0024】これらの処理に対応して、外部機器7においては、復調回路44において、伝送路を介して入力される暗号化データを復号する。また演算処理回路等により構成される制御部45より暗号キー変換回路46に指紋照合装置1と同一のパラメータK、Bを設定し、指紋照合装置1と同一の暗号キーQを作成する。またデスクランブル回路47において、復調回路44より出力される暗号化データをこの暗号キーQによりデスクランブル処理し、元のメッセージP2を復号する。さらに制御部45において、これらのメッセージに付加された位置データに基づいて、メッセージ部のデータを選択入力し、これにより照合結果、制御コマンドに応答するステータスデータを取得する。

【0025】また外部機器7の制御部45において、同様に制御コマンド、この制御コマンドに付随するデータでなる照合対象の画像データによりメッセージ部を形成し、このメッセージ部に冗長データ、位置データ、ランダムデータを付加してメッセージP1を形成する。さらにスクランブル回路48において、このメッセージP1をスクランブル処理することにより、暗号化データM1(=Enc(Q, P1))を生成し、この暗号化データM1が変調回路49により変調されて指紋照合装置1に入力される。

【0026】指紋照合装置1において、復調回路51は、この外部機器7より伝送された暗号化データを復号し、続くデスクランブル回路52は、暗号キーQによりこの暗号化データM1を処理し、これにより元のメッセージP1(=Dec(Q, M1))を復号する。なおここでDec(Q, M1)は、暗号キーQにより暗号化データM1を復号する関数である。制御部3においては、このメッセージP1に付加された位置データを基準にして、メッセージ部を選択的に入力し、これにより外部機器7より送出された制御コマンド、照合対象の画像データを取得する。

【0027】(1-2) 暗号キーの更新

ところでこのようにして全ての入出力データを暗号化し、また同一のデータが伝送されないようにしても、継続した盗聴等により暗号キーQが第三者に取得される場合も考えられることにより、この実施の形態では、外部機器7の制御により、一定周期で図4に示す処理手順を実行し、これにより暗号キーQを更新する。

【0028】すなわち制御部3は、外部機器7よりメッセージが到来すると、ステップSP1よりステップSP2に移り、このメッセージを解析し、キー更新コマンドが入力されたか否かを判断する。ここで否定結果が得られると、制御部3は、ステップSP3に移り、対応する処理手順を実行した後、ステップSP4に移ってこの処理

手順を終了する。

【0029】これに対して受信した制御コマンドがキー更新コマンドの場合、制御部3は、ステップSP2からステップSP5に移り、パラメータKの更新コマンドか否かを判断する。ここでこの実施の形態において、外部機器7は、図1について上述した暗号キーQの生成に必要なパラメータK又はBを、キー更新の制御コマンドと共に、図3のフォーマットにより伝送する。

【0030】制御部3は、このステップSP5において、肯定結果が得られると、ステップSP6に移り、パラメータKを取得して暗号キー生成回路41にセットし、続くステップSP7においてこの暗号キー生成回路41で生成される暗号キーQを更新する。これに応動して外部機器7においては、同様の処理を実行し、この指紋照合装置1と同一の暗号キーQをセットする。なお指紋照合装置1及び外部機器7においては、デフォルトのパラメータK及びBを有し、これにより例えば設置直後においては、このデフォルトのパラメータK及びBにより通信して、このシステム固有の暗号キーを設定するようになされている。

【0031】これに対してステップSP5において、否定結果が得られると、この場合入力された制御コマンドがパラメータBの更新コマンドでなることにより、制御部3は、ステップSP8に移り、パラメータBを取得して暗号キー生成回路41にセットし、続くステップSP7においてこの暗号キー生成回路41で生成される暗号キーQを更新する。これに応動して外部機器7においては、同様の処理を実行し、この指紋照合装置1と同一の暗号キーQをセットする。

【0032】(2) 実施の形態の動作

以上の構成において、指紋照合装置1は(図1)、所定の操作子の操作により、指紋読み取り部4において照合対象でなる指紋の画像が取得され、画像照合部5のデータベースに登録された基準画像とこの指紋の画像とが照合され、入出力部6を介して照合結果が外部機器7に出力される。また同様に、外部機器7より入力される制御コマンドに反応して、指紋読み取り部4において照合対象でなる指紋の画像が取得され、画像照合部5のデータベースに登録された基準画像とこの指紋の画像とが照合され、入出力部6を介して照合結果が外部機器7に出力される。さらに外部機器7の制御コマンドに付加された画像データを照合対象の指紋画像に設定して、画像照合部5のデータベースに登録された基準画像とこの指紋の画像とが照合され、入出力部6を介して照合結果が外部機器7に出力される。

【0033】またこれらの処理の他に、所定の操作子の操作により、指紋読み取り部4において取得された指紋の画像が画像照合部5のデータベースに基準画像として登録され、また同様に、外部機器7の制御コマンドに付加された画像データが画像照合部5のデータベースに登

録される。

【0034】これらの処理において、指紋照合装置1においては、制御コマンドに応答するステータスデータ、照合結果のデータが外部機器7に送出され、また外部機器7からは、制御コマンド、制御コマンドに付随する画像データ等が指紋照合装置1に伝送される。

【0035】これらのデータは(図3)、所定のパケット構造によるメッセージP1、P2に形成された後、指紋照合装置1及び外部機器7で共通の暗号キーQにより各スクランブル回路42、48においてスクランブル処理され、暗号化されて伝送される。これにより指紋照合装置1では、セキュリティが確保される。

【0036】このようにしてパケット構造のメッセージP1、P2に形成される際に、これらのデータは、冗長なデータ、メッセージ部の位置を示す位置データ、ランダムなデータが付加されて一定のデータ量により形成され、これにより例えば同一の照合OKのメッセージを送出する場合でも、伝送の都度異なる暗号化データにより伝送対象に送出される。これによっても、この指紋照合装置1では、システムの信頼性が図られる。

【0037】このようにして暗号キーQにより暗号化して種々のデータを送受するにつき、このシステムに設定された一定の周期により、暗号キーQの更新処理が実行される(図4)。すなわち外部機器7より、暗号キーの生成に必要なパラメータK又はBがメッセージ部に割り当てられて、それまでの暗号キーQにより暗号化されて伝送される。さらにこのパラメータK又はBにより、それぞれ指紋照合装置1及び外部機器7において、暗号キーQが更新される。

【0038】これにより暗号キーQが解読された場合でも、新たな暗号キーQにより種々のデータを送受することができ、信頼性を向上することができる。またこのとき暗号キーQの生成に必要なパラメータのみ伝送し、暗号キー変換回路41、46による演算処理により暗号キーQを生成することにより、直接暗号キーQを伝送する場合に比して信頼性を向上することができる。

【0039】(3)実施の形態の効果

以上の構成によれば、暗号キーの生成に必要なパラメータの伝送により暗号キーを更新することにより、照合結果を含む種々のデータを暗号化して伝送するにつき、伝送路を介して実行される不正行為を有効に回避することができ、これによりこの種のシステムのセキュリティを向上することができる。

【0040】またこのとき、ランダムなデータ、位置データを付加してスクランブル処理してパラメータを伝送

することにより、このパラメータ自体の不正な取得をも低減することができ、その分さらに一段とセキュリティを向上することができる。

【0041】(4)他の実施の形態

なお上述の実施の形態においては、指紋読み取り手段で読み取る指紋画像だけでなく外部機器より入力される指紋画像を処理する場合について述べたが、本発明はこれに限らず、単に指紋読み取り手段で読み取る指紋画像を処理する場合にも広く適用することができる。

【0042】また上述の実施の形態においては、いわゆるSALTの手法を適用する場合について述べたが、本発明はこれに限らず、種々の手法により同一のデータを異なるデータにより伝送する場合に広く適用することができる。

【0043】さらに上述の実施の形態においては、本発明を指紋照合装置に適用する場合について述べたが、本発明はこれに限らず、例えば印影の照合装置、網膜の照合装置等に広く適用することができる。

【0044】また上述の実施の形態においては、本発明を指紋照合装置でなる画像照合装置に適用する場合について述べたが、本発明はこれに限らず、例えば音声認識による個人を識別して登録された個人か否か識別する音声照合装置等、入力手段を介して得られる個々のデータを基準データと比較して照合結果を出力する照合装置に広く適用することができる。

【0045】

【発明の効果】上述のように本発明によれば、照合結果等を暗号化して伝送するにつき、パラメータの伝送により暗号キーを更新することにより、システムのセキュリティを向上することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る指紋照合装置の入出力部を示すブロック図である。

【図2】図1の指紋照合装置を示すブロック図である。

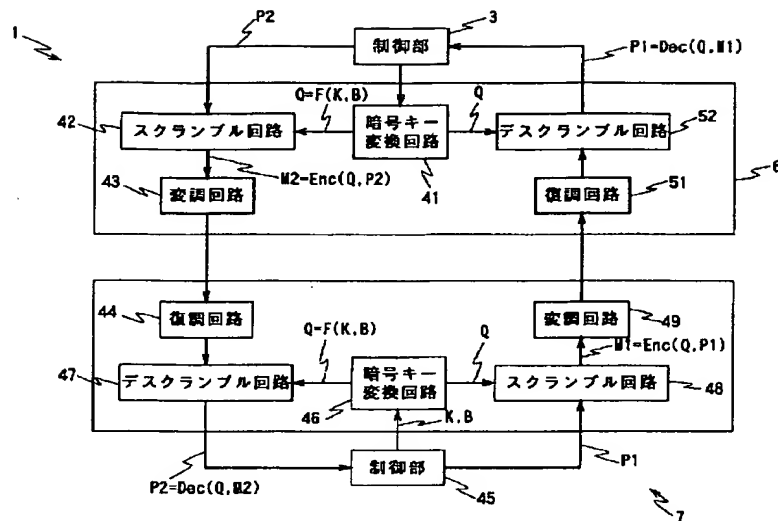
【図3】伝送に供するデータフォーマットの説明に供する略線図である。

【図4】暗号キーの更新処理の説明に供するフローチャートである。

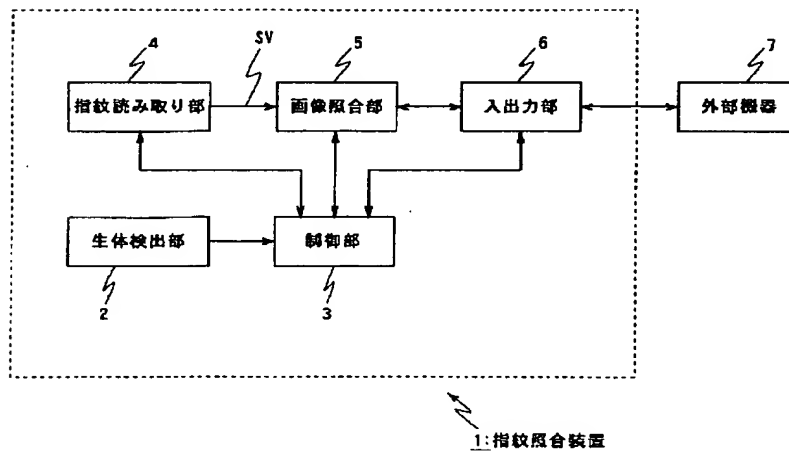
【符号の説明】

1……指紋照合装置、2……生体検出部、3……制御部、4……指紋読み取り部、5……画像照合部、6……入出力部、7……外部機器、41、46……暗号キー変換回路、42、48……スクランブル回路、47、52……デスクランブル回路

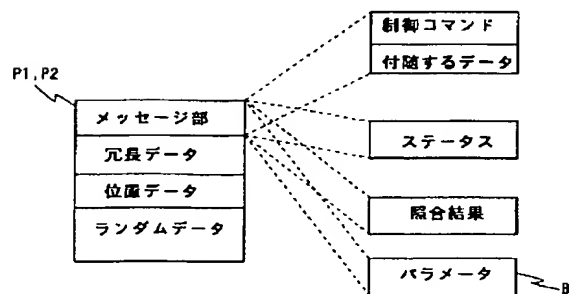
【図1】



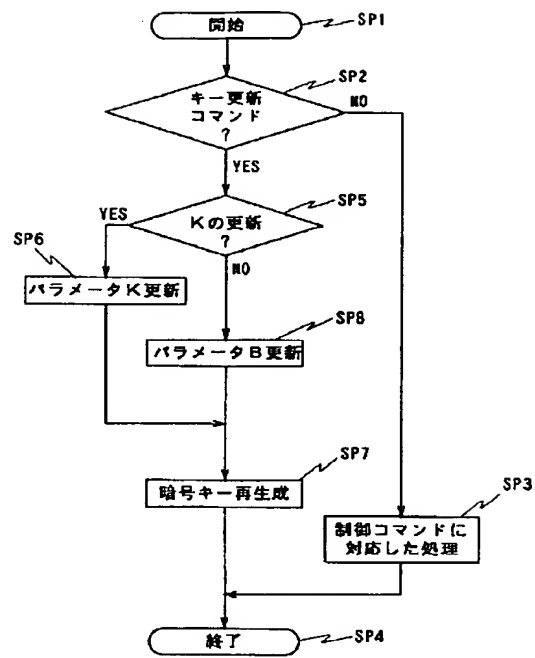
【図2】



【図3】



【図4】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.